

情報科学系セミナー(第4回)

テーマ

「同種写像暗号入門」

講演者: 三菱電機株式会社 情報技術総合研究所

主管技師長 高島 克幸

日時: 令和元年 8 月 8 日(木) 15:30~17:00

場所: 情報科学系講義棟2階 講義室 I3・4

講演要旨:

(大規模)量子計算機の出現に備えて、量子計算機を用いても破れない公開鍵暗号の研究が活発に行われている。本講演では、その候補である同種写像暗号について紹介する。その暗号演算には、同種写像からなるグラフ上のランダムウォークが使われており、例えば、超特異曲線同種写像から得られるラマヌジャングラフの数理的な性質が、暗号の性能・安全性を理解する上で重要になる。それら数理的側面と共に、同種写像を使った鍵共有や署名方式についても紹介する。

講演者略歴:

1993年	京都大学理学部 卒業
1995年	京都大学大学院 理学研究科 数学・数理解析専攻 博士前期課程修了
1997年	三菱電機株式会社 入社
2009年	京都大学大学院 情報学研究科 社会情報学専攻 博士後期課程修了(情報学博士)
2013年	九州大学マス・フォア・インダストリ研究所 客員教員
2016-2017年度	日本応用数理学会副会長

参加申込・予約は不要です。直接会場にお越しください。

お問合せ先: 共通事務管理課共通事務第二係 (E-mail: is-secr)